DEPARTMENT OF DEFENSE

PHYSICAL SECURITY ENTERPRISE & ANALYSIS GROUP

PSEAG

2015 RDT&E

RESEARCH, DEVELOPMENT, TEST & EVALUATION

PROGRAM SUMMARY

PSEAG

Contents

Introduction

Decision Support

Detection & Assessment

Installation & Transport Security

Prevention

Storage & Safeguards

APPENDICES

Introduction

Department of Defense Physical Security Research, Development, Test and Evaluation (RDT&E) Program Overview

The Department of Defense (DoD) Physical Security Research, Development, Test and Evaluation (RDT&E) Program provides physical security equipment and analyses to meet the immediate and projected force protection challenges of the Services and the combatant commands. The PSE RDT&E Program is supported by three Thrust Areas through which the DoD and PSEAG focus their physical security activities:

Conventional Physical Security

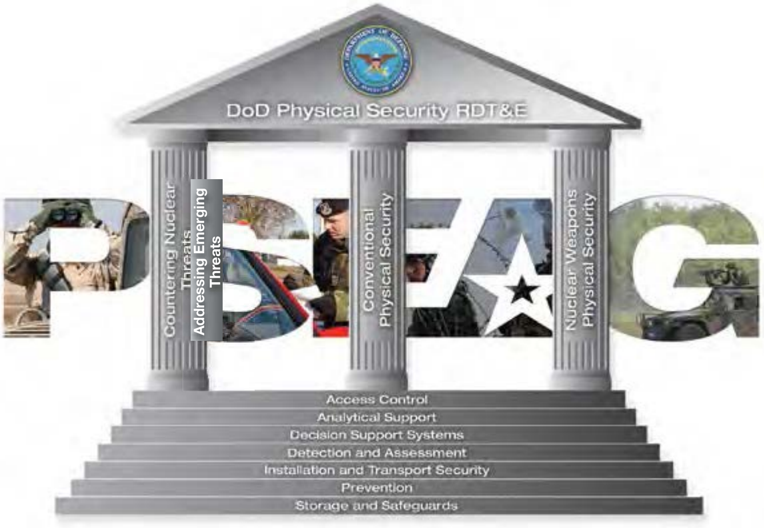
Protection of personnel; prevention of unauthorized access to non-nuclear weapons equipment, installations, materials, and documents; and, safeguarding of the foregoing against espionage, sabotage, damage, and theft.

Nuclear Weapons Physical Security

Protection of nuclear weapons, and related equipment, installations, materials, and documents; and safeguarding of the foregoing against espionage, sabotage, damage, and theft.

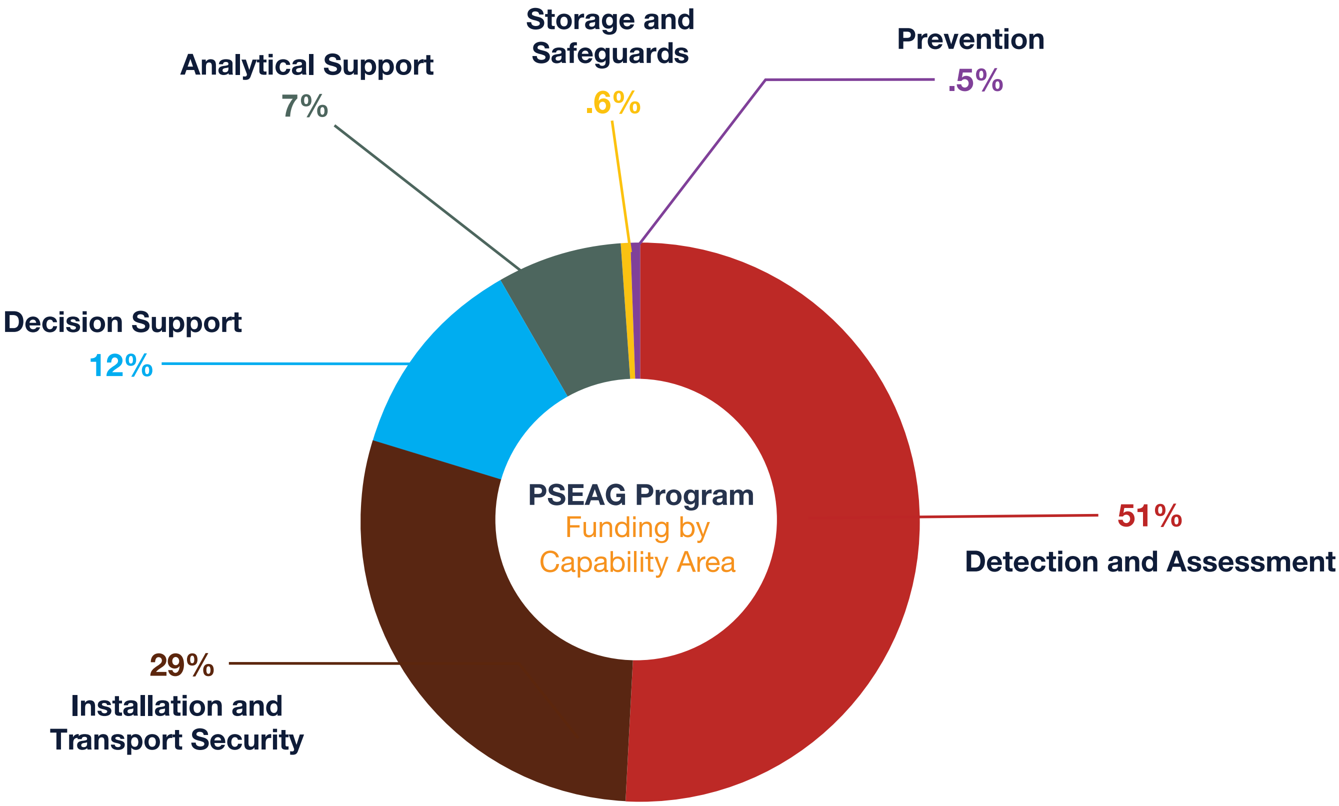
Underpinning this entire structure is a foundation of physical security activities, which are now organized into capability areas, centered on key physical security requirements. These capability areas bring together formerly disparate physical security projects into more cohesive and synergistic physical security programs, each with identifiable benefits and results for the end-user:

- Access Control
- Analytical Support
- Decision Support Systems
- Detection and Assessment
- Installation and Transport Security
- Prevention
- Storage and Safeguards


DoD Physical Security RDT&E
Countering Nuclear Threats
Addressing Emerging Threats
Conventional Physical Security
Nuclear Weapons Physical Security
PSEAG
Access Control
Analytical Support
Decision Support Systems
Detection and Assessment
Installation and Transport Security
Prevention
Storage and Safeguards

PSEAG Program Funding by Capability Area

Similar to previous years, Detection and Assessment is the largest capability area in the program for funding. In 2015, Installationand and Transport Security became the second largest capability area for funding due to Service priorities and requirements



Decision Support

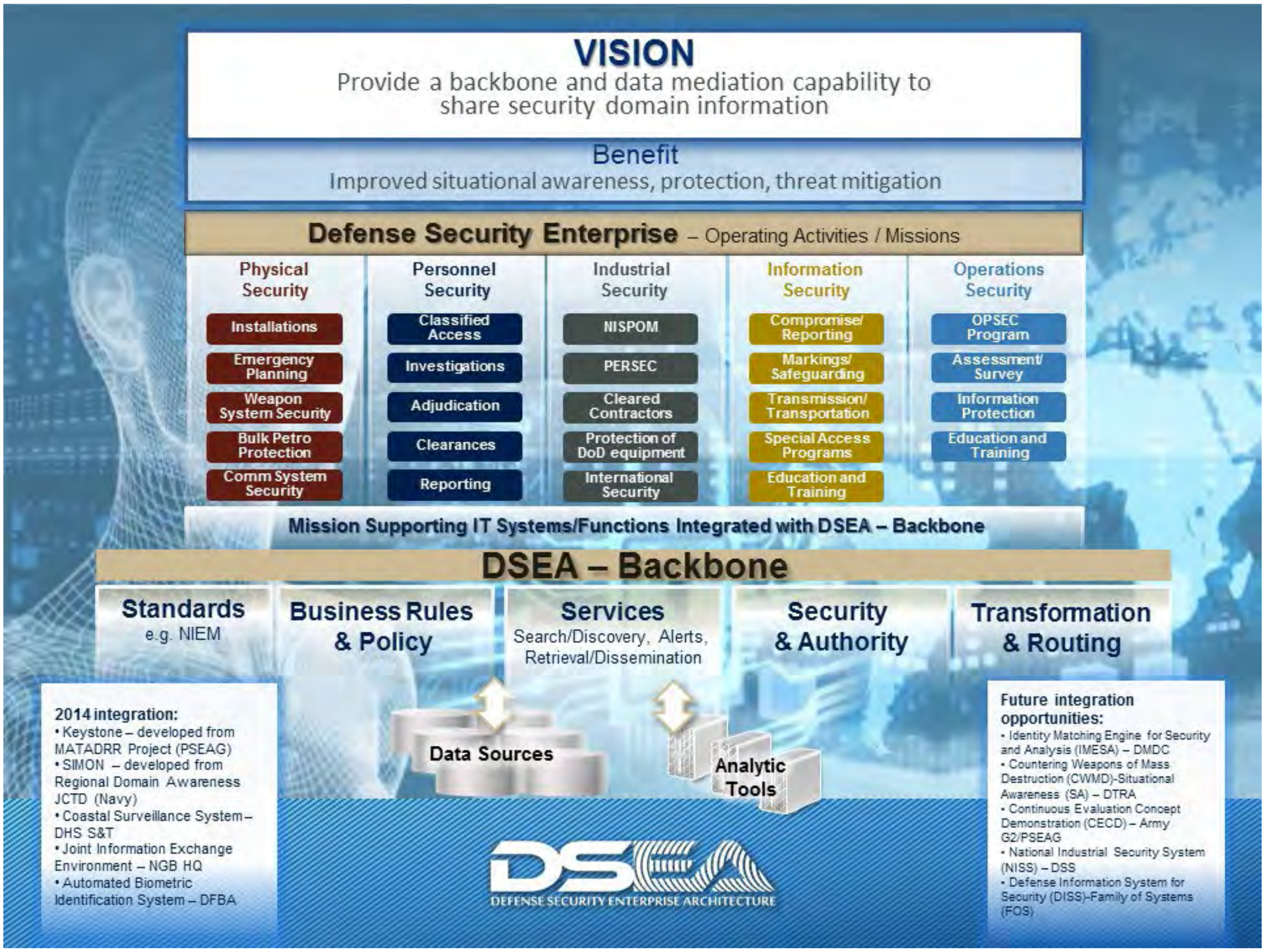
Decision support systems serve the management, operations, and planning levels of the DoD physical security enterprise to help make decisions, which may be rapidly changing and not easily specified in advance. This capability area focuses on command and control equipment and projects related to the creation and enhancement of common operating pictures, and the establishment of common architectures / interface standards.

Defense Security Enterprise Architecture

Shared and automated content across the security domains and functional areas, enabling more efficient and accurate personnel vetting, access controls, insider threat prevention and enhanced security operating environments.

Requirements

- Homeland Security Presidential Directive (HSPD)-5
- HSPD-12
- Ft Hood Report Findings and Recommendations
- DoDD 5200.43; Management of the Defense Security Enterprise



VISION

Provide a backbone and data mediation capability to share security domain information

Benefit

Improved situational awareness, protection, threat mitigation

Defense Security Enterprise – Operating Activities / Missions

Physical Security	Personnel Security	Industrial Security	Information Security	Operations Security
Installations	Classified Access	NISPOM	Compromise/ Reporting	OPSEC Program
Emergency Planning	Investigations	PERSEC	Markings/ Safeguarding	Assessment/ Survey
Weapon System Security	Adjudication	Cleared Contractors	Transmission/ Transportation	Information Protection
Bulk Petro Protection	Clearances	Protection of DoD equipment	Special Access Programs	Education and Training
Comm System Security	Reporting	International Security	Education and Training	

Mission Supporting IT Systems/Functions Integrated with DSEA – Backbone

DSEA – Backbone

Standards
e.g. NIEM

Business Rules & Policy

Services
Search/Discovery, Alerts, Retrieval/Dissemination

Security & Authority

Transformation & Routing

2014 integration:
- Keystone – developed from MATADRR Project (PSEAG)
- SIMON – developed from Regional Domain Awareness JCTD (Navy)
- Coastal Surveillance System – DHS S&T
- Joint Information Exchange Environment – NGB HQ
- Automated Biometric Identification System – DFBA

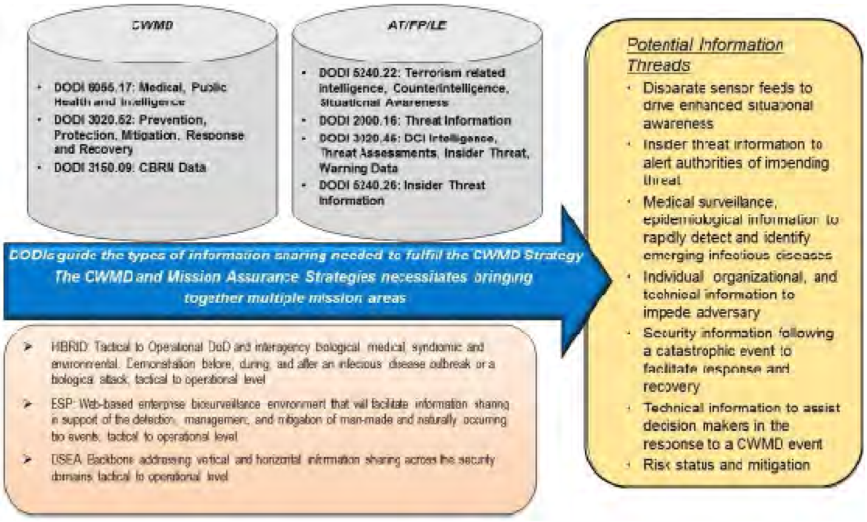
Data Sources

Analytic Tools

Future integration opportunities:
- Identity Matching Engine for Security and Analysis (IMESA) – DMDC
- Countering Weapons of Mass Destruction (CWMD)-Situational Awareness (SA) – DTRA
- Continuous Evaluation Concept Demonstration (CECD) – Army G2/PSEAG
- National Industrial Security System (NISS) – DSS
- Defense Information System for Security (DISS)-Family of Systems (FOS)

Defense Security/Chemical, Biological, Radiological and Nuclear (CBRN) Information Analysis

Identification, evaluation, and selection of specific information and data integration points between the CWMD and Defense Security Communities based on gaps and opportunities identified and illustrate how multiple disparate domains can be connected for critical improvement in preparation and response to conventional and CBRN events.



CWMD

- DODI 6055.17: Medical, Public Health and Intelligence
- DODI 3020.52: Prevention, Protection, Mitigation, Response and Recovery
- DODI 3150.09: CBRN Data

AT/FP/LE

- DODI 5240.22: Terrorism related intelligence, Counterintelligence, Situational Awareness
- DODI 2000.16: Threat Information
- DODI 3020.46: DCI Intelligence, Threat Assessments, Insider Threat, Warning Data
- DODI 5240.26: Insider Threat Information

DODIs guide the types of information sharing needed to fulfill the CWMD Strategy

The CWMD and Mission Assurance Strategies necessiates bringing together multiple mission areas

- HBRID: Tactical to Operational DoD and interagency biological, medical, syndromic and environmental. Demonstration before, during, and after an infectious disease outbreak or a biological attack, tactical to operational level
- ESP: Web-based enterprise biosurveillance environment that will facilitate information sharing in support of the detection, management, and mitigation of man-made and naturally occurring bio events, tactical to operational level
- DSEA Backbone addressing vertical and horizontal information sharing across the security domains tactical to operational level

Potential Information Threads

- Disparate sensor feeds to drive enhanced situational awareness
- Insider threat information to alert authorities of impending threat
- Medical surveillance, epidemiological information to rapidly detect and identify emerging infectious diseases
- Individual organizational, and technical information to impede adversary
- Security information following a catastrophic event to facilitate response and recovery
- Technical information to assist decision makers in the response to a CWMD event
- Risk status and mitigation

Requirements

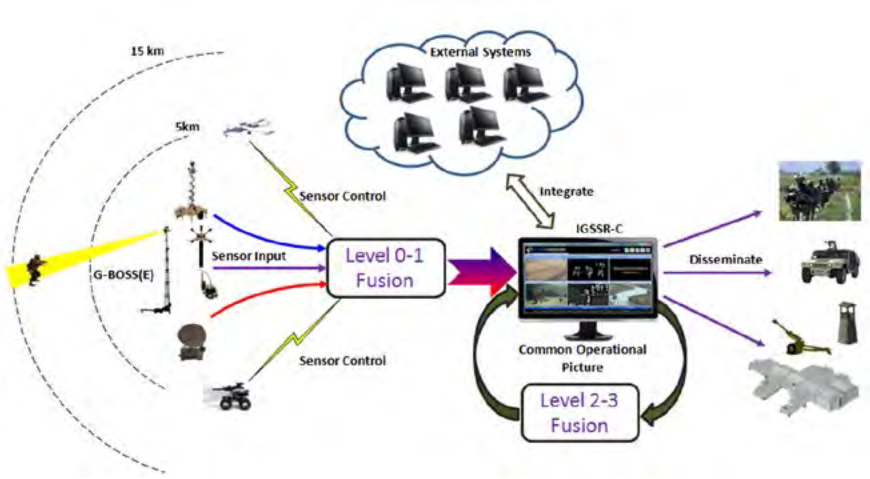
- Service Requirements: NORTHCOM (NC) FY 16-20 Integrated Priority List (IPL) Priority 9: Info Sharing
- NC FY 16-20 Science and Technology Integrated Priority List (STIPL) Priority 15: Force Protection Condition (FPCON) & Threat Info Coordination
- EUCOM (EC) FY16-20 IPL Priority 4: Information Sharing Policies, Procedures
- Supporting Requirements Documents: HSPD 5, 8, and 10; Quadrennial Homeland Security Review; DoDD 5200.43, Defense Security Enterprise; Washington Navy Yard (WNY) Report; Various Policy, Initial Capabilities Documents (ICD), Capabilities Development Documents (CDD), and Capability Production Document (CPD)

Requirements

- Interoperability ICD Approved (CARDS 1052) - Mar 2010; IGSSR-C CDD Approved (CARDS 6093) - Sep 2013

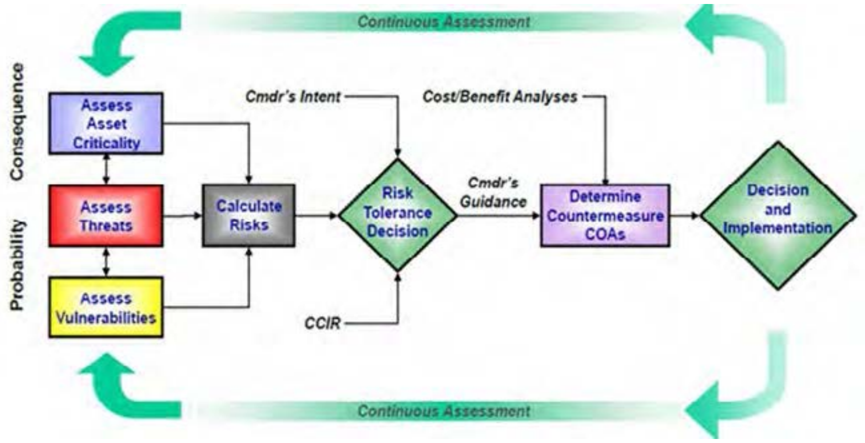
Integrated Ground Security, Surveillance and Response Capability

This project provided a layered approach to integrate sensors, sensor systems, and unmanned systems and obtained automated fusion to create an in-depth security, surveillance and response Force Protection Common Operational Picture capability for fixed, semi-fixed, or expeditionary elements in all operating environments. IGSSR-C's key component is a suite of software that achieves integration, fusion, and interoperability.



Joint Risk Decision Support Tool

The overall effort will develop an enterprise installation decision support initiative application providing risk analysis and risk mitigation decision support in a secure, web-enabled architecture to be hosted on the DoD's SIPRNET. Adapting the capabilities of the Air Force's and Army's ForcePRO software tool, this new application supports all services and results in a standardized Service and Major Command roll-up for expanded visibility of the risk picture and for more fiscally efficient procurement of necessary resources. The project also includes a requirements definition study and software development program to address All Hazards and Mission Assurance (MA) areas.

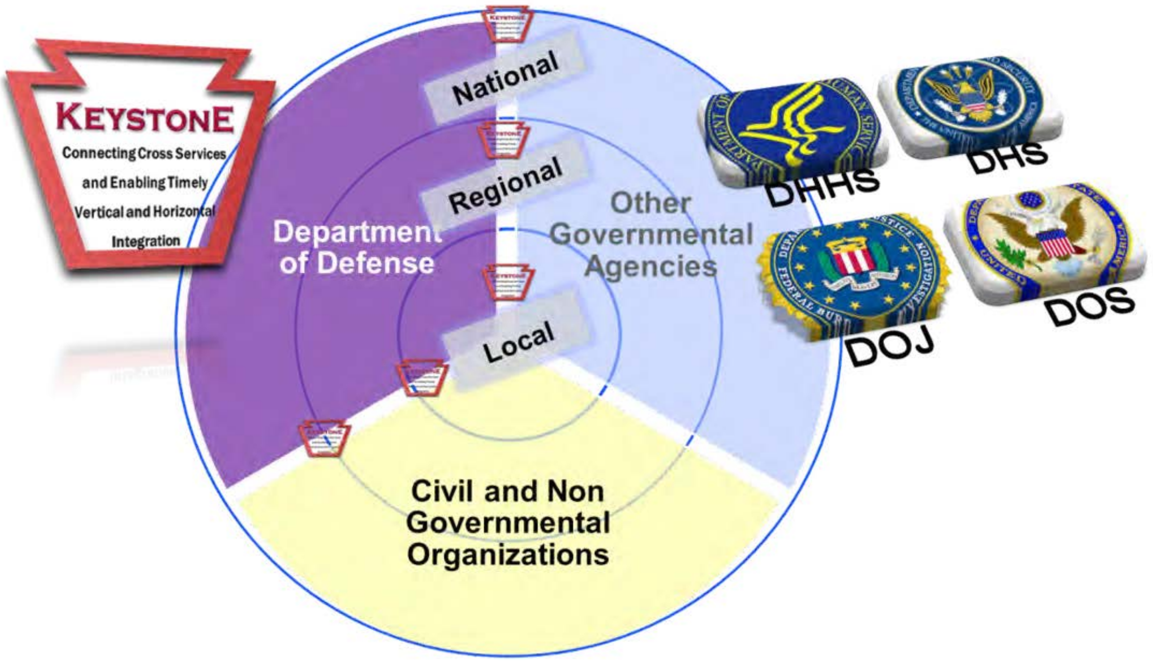


Requirements

- 2015 DoD Mission Assurance Assessment Benchmarks;
- DoD Mission Assurance Strategy, 7 May 2012

Keystone Phase II (Discovery) Analysis Humanitarian Aid/Disaster Relief

The intent of this project is a discovery phase to determine requirements for further analysis and to build partnerships with the Emergency Management community. The Keystone Phase II analysis will identify applications from both the Host Nation support communities (e.g. NATO and Red Cross) and US Combatant Commands that would benefit from an allied capability to integrate and correlate collection, analysis, reporting, and processing of OCONUS Humanitarian Aid/Disaster Relief emergency management, force protection and threat information.

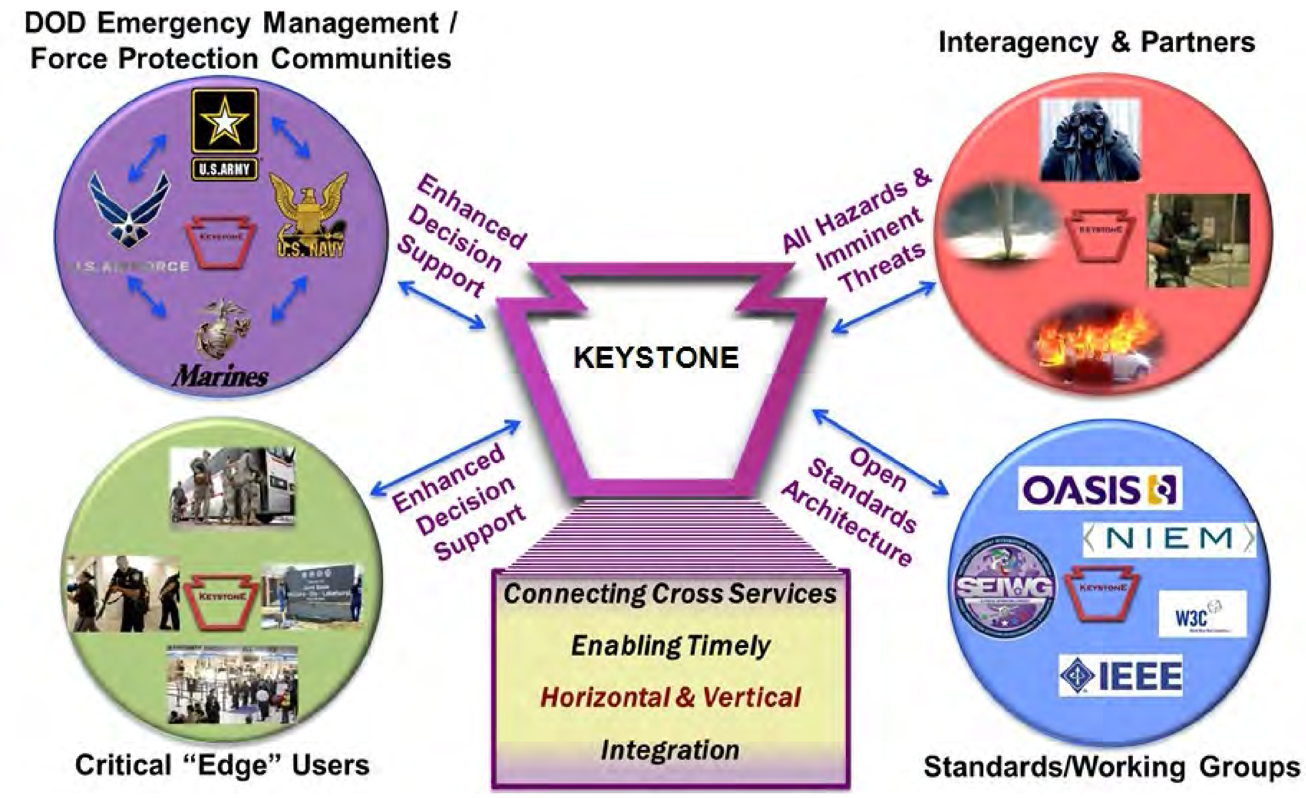

KEYSTONE
Connecting Cross Services and Enabling Timely Vertical and Horizontal Integration
National
Regional
Local
Department of Defense
Other Governmental Agencies
Civil and Non Governmental Organizations
DHHS
DHS
DOJ
DOS

Keystone United States European Command Technical Demonstration

This demonstration identified applications from both the German Host Nation first responders and United States Army Garrison Stuttgart to form an allied capability to integrate and correlate collection, analysis, reporting, and processing of OCONUS emergency management, force protection, and threat information from existing systems. The integration software and user-level equipment demonstrated information sharing, a proof-of-concept integration of German Host Nation systems, and software/cloud hosting to avoid creating a new stovepipe or need for new equipment.

Requirements

- Final Recommendations of the Fort Hood Follow on Review" dated 18 Aug 2010; Washington Navy Yard Shooting Findings
- EUCOM IPL #5

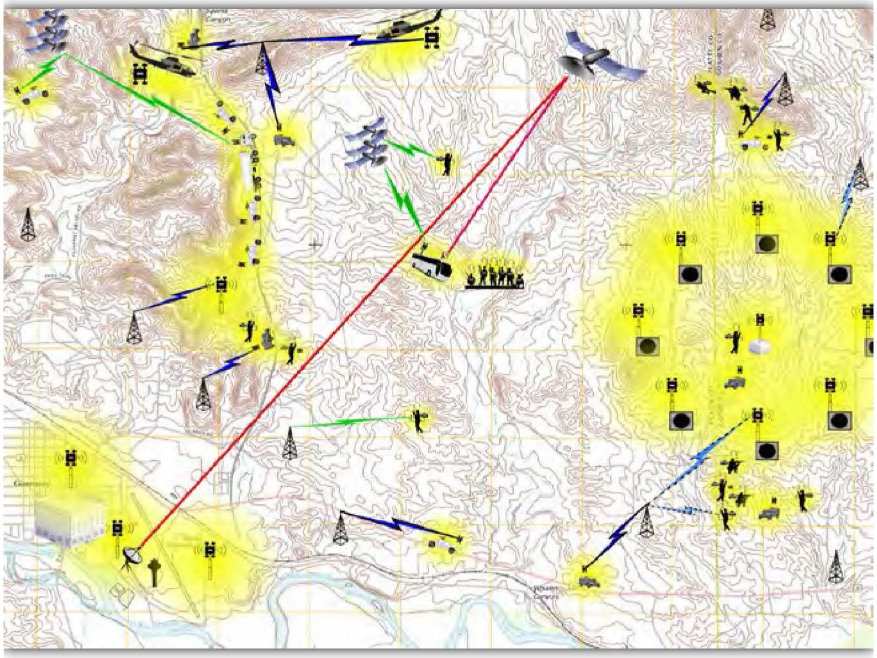


Requirements

- USAF Nuclear Security Roadmaps Needs, Mighty Guardian Results, Increase in security operations efficiencies

Defense Force Command, Control, Communications, and Situational Awareness

This project provides a redundant combination of physical and software application layers to provide a fail-safe communications capability for stationary and on-the-move assets in the missile field (including blue force tracking).



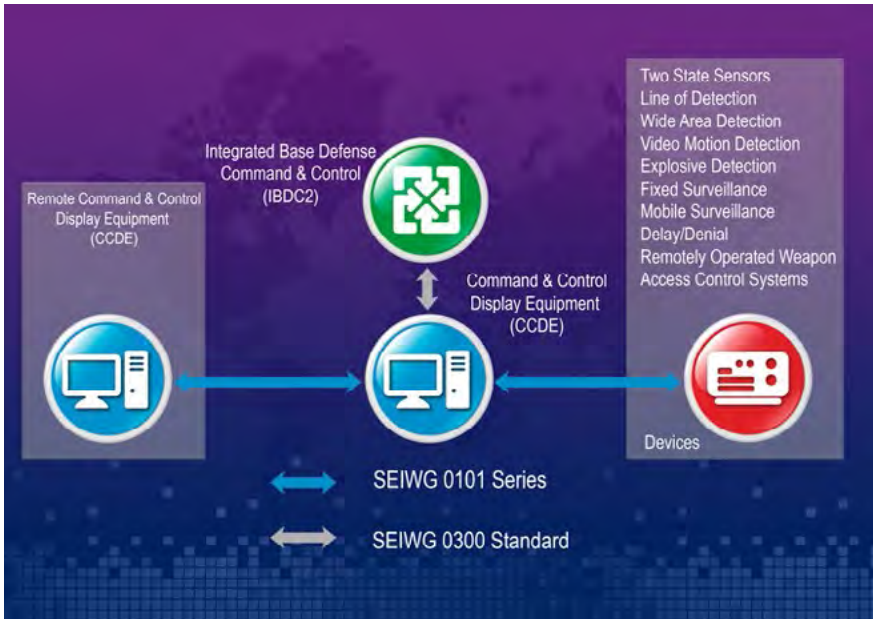
Security Equipment Integration Working Group

The SEIWG provides the support necessary to carry out the SEIWG Letter of Instruction, including technical/SME support to the Defense Security Enterprise Discovery (DSED) efforts, attending review/planning meetings, developing and updating Interoperability Standards, coordinating SEIWG products within the Joint Services/components, working with other standards working groups to maintain the DoD influence on PSE, and providing technical reviews and development of joint PSE architecture products in direct support of PSEAG funded initiatives.

In FY 15, the SEIWG embarked on developing a National Information Exchange Model (NIEM) Information Exchange Package Document (IEPD) that fully encompasses the message exchanges specified within the SEIWG 0101C Interoperability Standard. NIEM is a community-driven, government-wide, standards-based approach to exchanging information.

The NIEM MILOps (Military Operations) domain was established in 2013. In August 2015, Department of Defense Instruction (DoDI) 8320.07 was released and contains DOD policy that "…(NIEM)-based exchanges must be considered for all new Extensible Markup Language (XML) information exchanges created and for all XML information exchanges being modernized as part of the normal lifecycle management for these information exchanges."

In support of DODI 8320.07, the PSEAG sponsored this forward-focused development effort to provide information-sharing solutions that assist the Joint Services also here in meeting their future mission and operational needs. The resultant NIEM IEPD is anticipated to be released 2Q-FY17.



Requirements

- DoDI 3224.03 dated 1 Oct 2007, section 6.4.2.4.
- DoDI 8320.07 dated 3 Aug 2015, section 3.b.

Detection & Assessment

The ability to detect adversaries and assess their intentions is a basic physical security tenant. This capability area focuses on deficiencies in equipment used to identify and warn of unauthorized access to a specified area or installation as well as equipment related to the notification and identification of explosive threats or hazards.

Comparative Evaluation of Trace Detection Systems for Use at an Entry Control Point

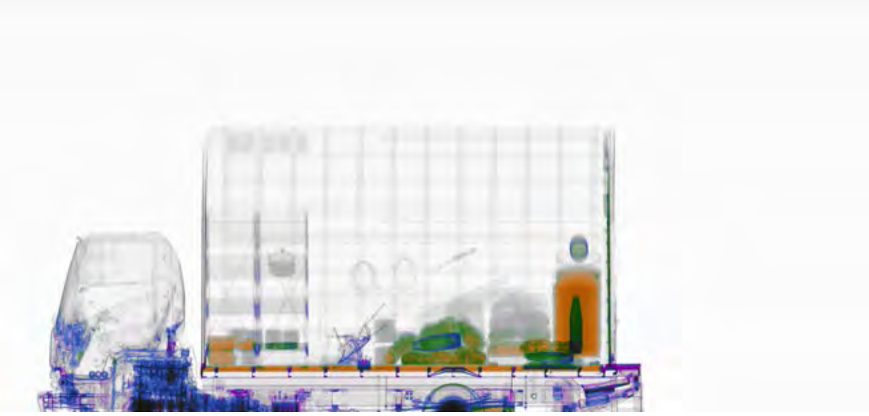
This effort is an assessment of the currently available commercial-off-the-shelf trace explosive detection systems, specifically those that could be employed at an entry control point.

Requirements

- Joint Urgent Operational Needs Statement CC-0255
- Improvised Explosive Device Defeat ICD
- Navy Urgent Operational Needs Statement Chemical, Biological, Radiological, Nuclear, and Explosives (CBRNE)
- Integrated Base Defense Security System CDD
- Integrated Unit, Base Installation Protection ICD
- Joint Service Explosive Ordnance Disposal ICD
- Notional Concept 07-07

Dual Energy X-Ray Vehicle Imaging Comparative

The objective of this effort is to complete a comparative test and evaluation of up to five recently developed dual energy vehicle x-ray imaging systems. A final report of findings from the test and evaluation will be published and will provide recently developed recommendations as to the limitations, capabilities, and utility of the systems.



Requirements

- CENTCOM 2013 IPL 7 (STIPL 6.c & 6.u)
- Fleet Forces Command (FFC) 2011 IPCL 1,3, & 6
- Integrated Base Defense Security System (IBDSS) CDD Feb 2005 B.2
- Integrated Unit, Base, Installation Protection (IUBIP) ICD Jan 2008; DoDI 2000.16, Antiterrorism Program, Oct 2006

Explosive Detection Equipment (EDE) for Maritime Environment

The primary objective of this effort is to establish the capabilities and limitations of explosive detection systems and identify the system that most effectively meets the requirements set forth by Fleet Forces Command for use in maritime theaters of operation.

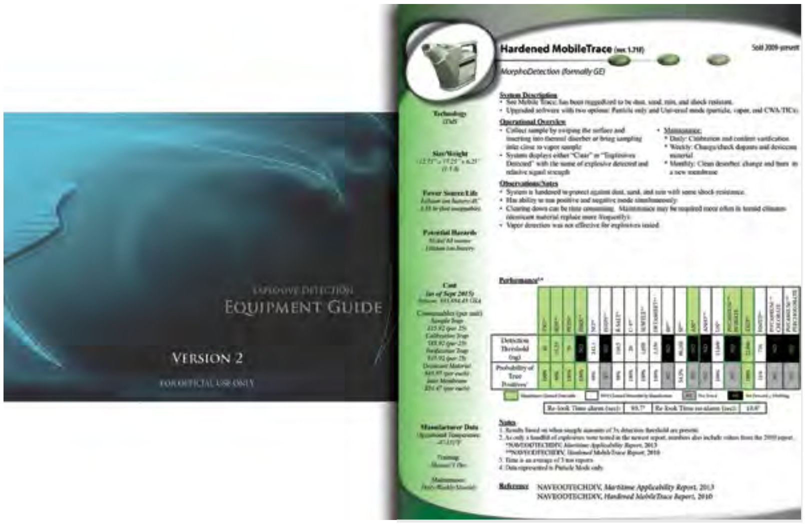
Requirements

- Joint Urgent Operational Needs Statement CC-0490
- Integrated Unit, Base Installation Protection ICD
- Joint Urgent Operational Needs Statement CC-0255
- Improvised Explosive Device Defeat ICD
- Portable CBRNE/Weapons of Mass Destruction Detector, Navy Urgent Operational Needs Statement
- Integrated Base Defense Security System CDD
- Joint Service Explosive Ordnance Disposal ICD
- CBRNE Sense ICD

Explosive Detection Equipment Guide version 2.0 and Selection App

Requirements
- PSEAG Capability Gap 4

This project will update EDE Guide version 1.0 to focus on the acquisition community and include updated data on new systems. This effort will also include the development of an App for assisting both users and the acquisition community with selecting EDE for their applications/needs.



Requirements

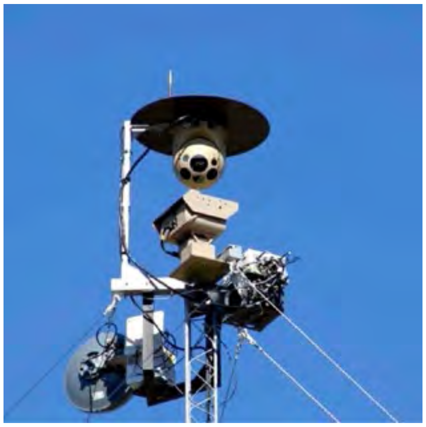
- DoD S5210.41M

Foliage Penetration Technology Evaluation

This project seeks to identify, evaluate, and further develop the most promising technologies for assessing human activity within heavily forested areas from ground level.

Ground-Based Operational Surveillance System (Expeditionary)

This project provides persistent surveillance to support various base camp sizes, outpost, and Military Police Combat Support Companies. The capability is an expeditionary, ground-based, self-contained, multi-spectral sensor-oriented, persistent surveillance system used to greatly enhance situational awareness to counter physical security threats.



Requirements

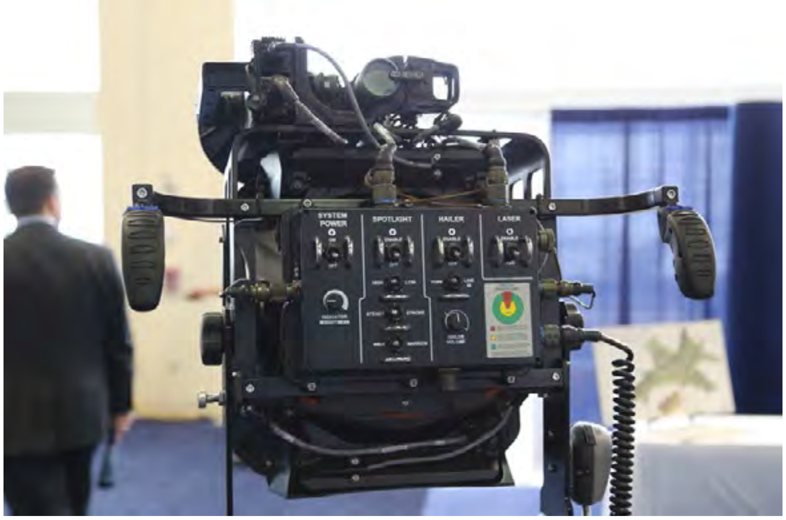
- Capability Development Document for G-BOSS(E), Version 4.0, J8, 15 Mar 2012
- Training and Doctrine Command (TRADOC) validation of Army Annex to adopt USMC G-BOSS(E) CDD, 19 Aug 2013
- Headquarters, Department of the Army (HQDA) Deputy Chief of Staff G3/5/7 approved USMC G-BOSS(E) CDD adoption, designation as Joint Integration with CARD number is 06099, 6 May 2014

Hailing Acoustic, Laser, and Light Tactical System

This project provides a single operator with the ability to simultaneously control and operate multiple non-lethal deterrent devices to guard checkpoints, keep-out zones, and ship close-aboard areas.

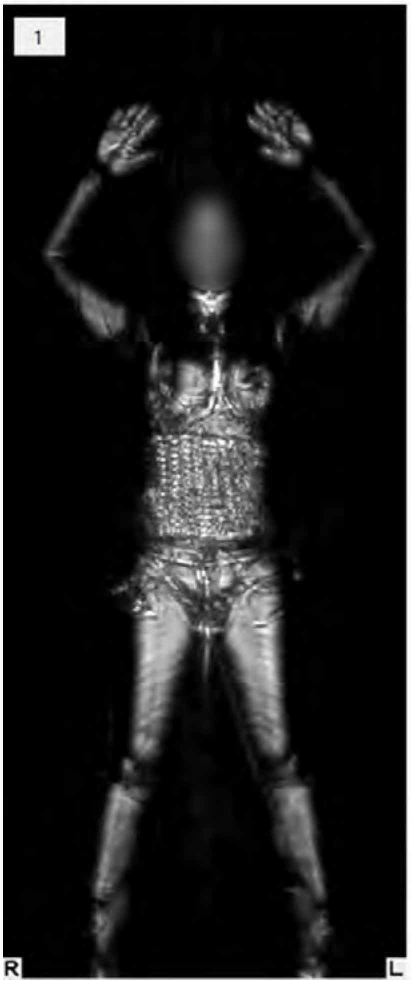
Requirements

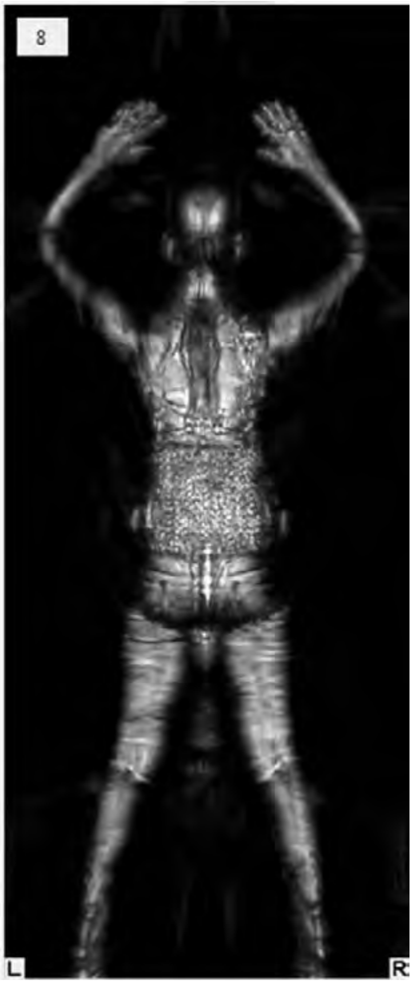
- UONS #9309 [Counter Swarm]; UONS #9313 [Non-Lethal Weapons]; Request for Information (RFI) N00178-11-Q-3900



Millimeter Wave Asymmetric Threat Detection

This effort will evaluate two widely-used commercial millimeter wave personnel screening systems and their capability to detect certain bulk explosive arrangements when worn by a human subject. Previous testing of similar personnel screening systems revealed potential detection limitations of these types of threats.



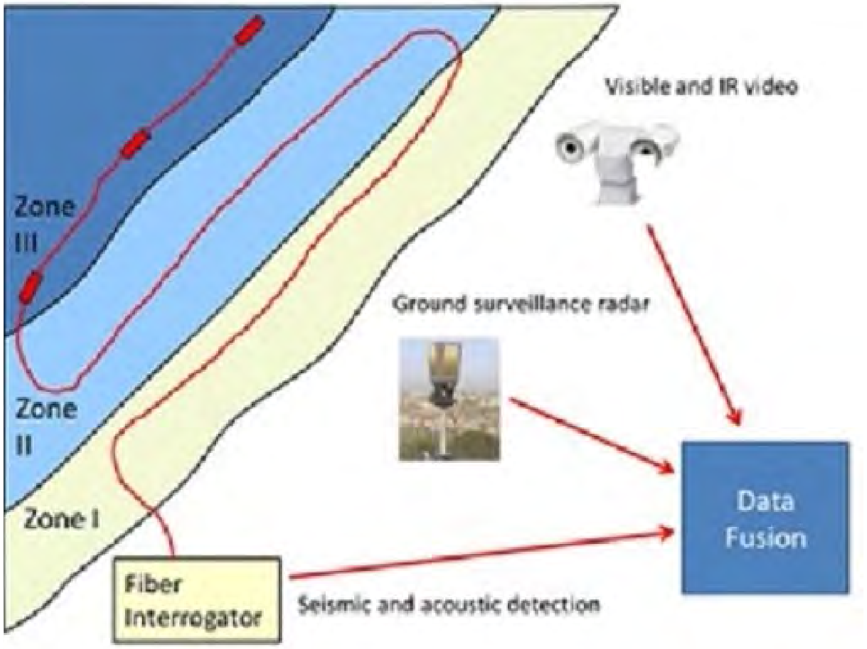


Requirements

- CENTCOM 2013 IPL 7 (STIPL 6.c & 6.u)
- FFC 2011 IPCL 1,3, & 6
- IBDSS CDD Feb 2005 B.2
- IUBIP ICD Jan 2008
- DoD 2000.16 Oct 2006

Multi-sensor Detection and Discrimination

This project is developing a scalable multi-sensor wide area surveillance system deployed at the land-water interface (LWI) for autonomous detection and discrimination of asymmetric threats with no coverage gaps. The system's objective is to provide consistent threat detection and accurate threat assessment at LWI.



Radar Assisted Area Protection

This project is testing and developing of Interferometer radar technology to advance the capability to search, detect, track, and identify Rocket Propelled Grenades, Anti-tank Guided Missiles, and Unmanned Aircraft Systems and direct-fire standoff threats for installation and asset defense.

Requirements

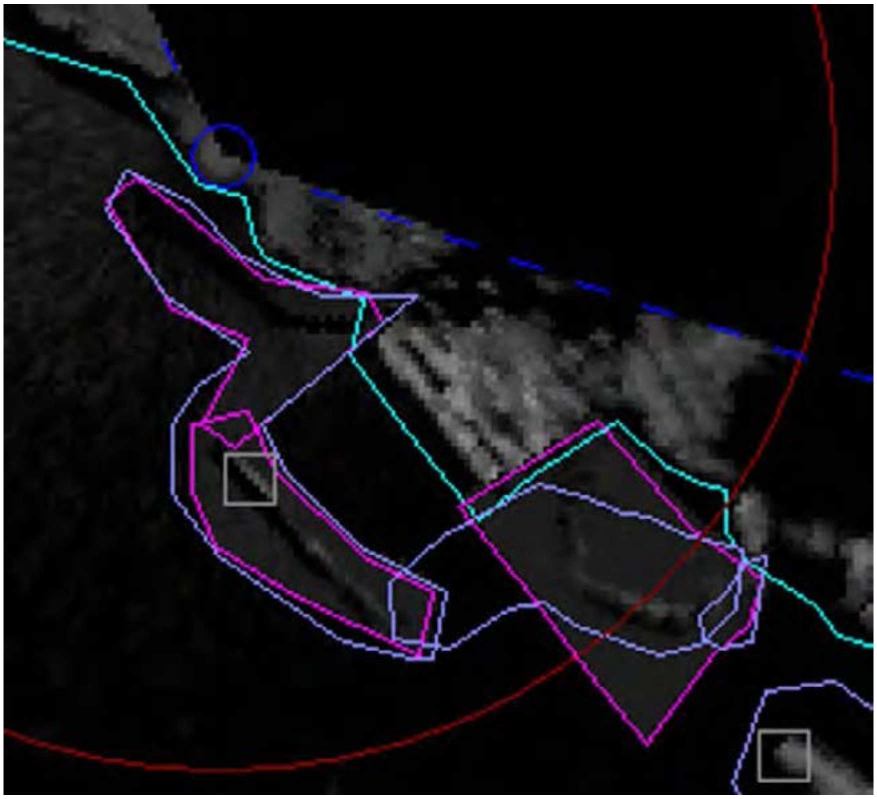
- DoD S5210.41-M

Requirements

- Electronic Harbor Security Systems (EHSS) CONOPS
- EHSS Key System Attributes
- EHSS ICD

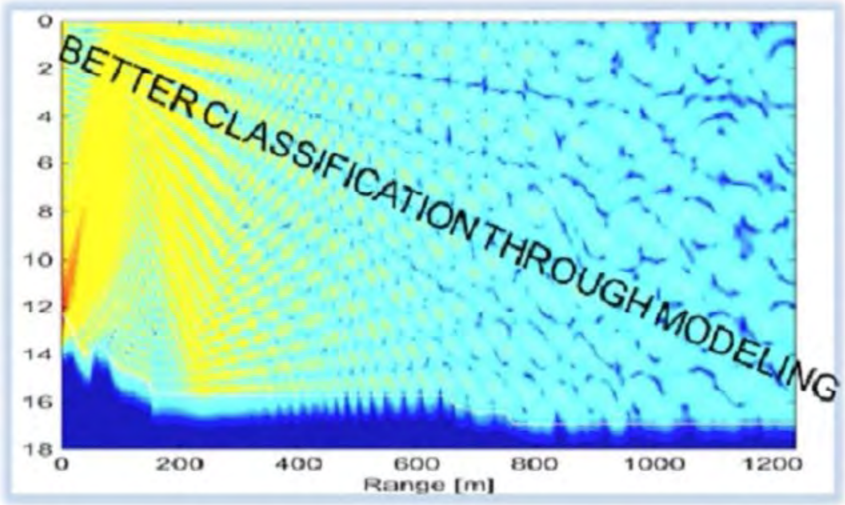
Radar Processing Dynamic Structure Filter

This project will develop new techniques and algorithms using established processes (lower risk) to automate the filtering of permanent and/or semi-permanent floating structures detected by the Electronic Harbor Security System.



Sonar Propagation Acoustic Model Transition to Operational Initial Capability

This project will reduce false alarms from sonars at operational sites by employing adaptive classification based on modeled acoustics.

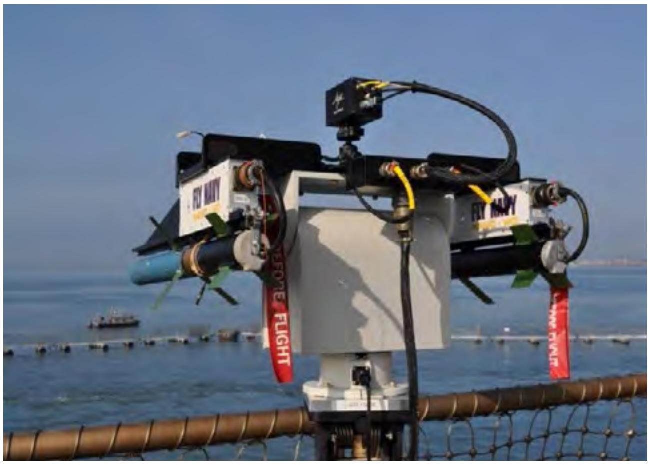


Requirements

- DoD S5210.41M (2009), Vol 3, para 8.d.(3)

US Navy Spike Weapon System Electro-Optical Seeker Upgrade

This project is developing and demonstrating an improved electro-optical seeker that will enable the Spike Weapon system to reliably track and engage AntiTerrorism / Force Protection (AT/FP) stationary and moving threat targets while operating in complex shorefront environments during day and low light conditions.



Requirements

- Deputy Secretary of Defense (DEPSECDEF) Memorandum, 23 Jun 2012, "USCENTCOM/ USPACOM Capability Enhancements"
- Commander, US FFC Memorandum, 22 Sep 2011, "2011 Fleet Antiterrorism/Force Protection IPCL"
- CENTCOM JUONS CC-0506 Title: Smart Munitions for Aerostat Target Designation

Installation & Transport Security

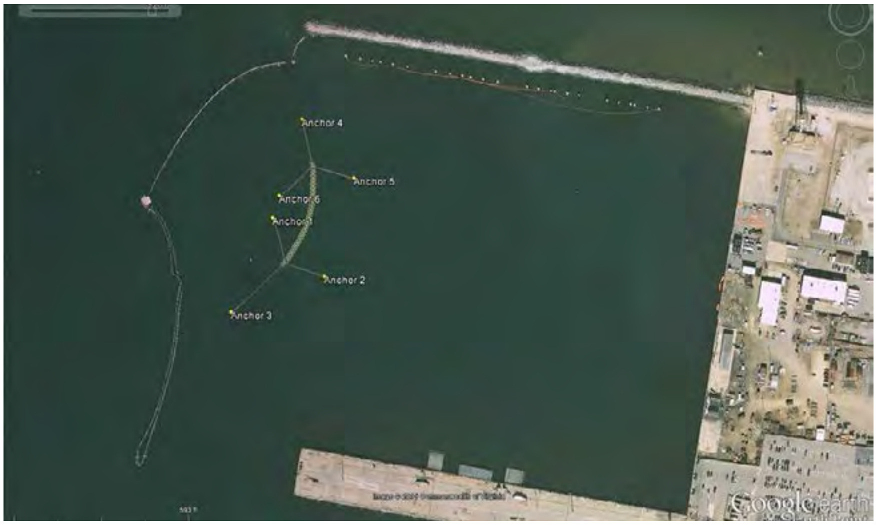
This capability area focuses on solutions to deficiencies in equipment intended to improve the physical security profile of fixed sites and facilities, as well as critical items while in-transit. Robust installation and transport security are vital to preventing a weapon of mass destruction attack or unauthorized access to key assets such as nuclear weapons and special nuclear material.

Requirements

- US Navy's Performance Specification for the AT/FP Boat Barriers dated 30 Aug 2009
- DoDI 2000.16, Antiterrorism Program Standards
- Secretary of the Navy Instruction 3300.2B, Department of Navy (DON) AT/FP Program
- Office of the Chief of Naval Operations (OPNAV) Instruction (OPNAVINST)
- Navy Antiterrorism Program
- OPNAVINST 3300.56
- Navy Combating Terrorism Program Standards
- OPNAVINST 5530.14E, Navy Physical Security and Law Enforcement Program
- NTTP 3-07-2-3, Navy Tactics, Techniques, and Procedures for Law Enforcement and Physical Security for Navy Installations

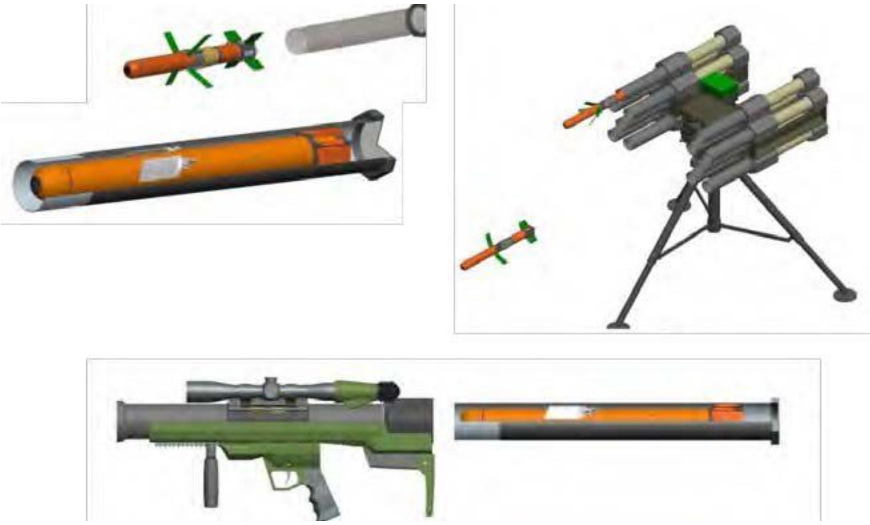
Automated Harbor Barrier Gate - Operational Suitability

This effort is a follow-on effort to the Integrated Waterside Security Concept Demonstration conducted in September 2014 to conduct a jointly funded Developmental Test (DT) of a Type II Water Barrier System at an operationally relevant site. The DT will consist of live testing of a water barrier system that is compliant with the US Navy's Performance Specification for the AT/FP Boat Barriers dated August 30, 2009. Under this task, a 300 foot gate section was delivered with moorings and a semi-automated gate.



US Navy Spike Weapon System, Common Launch Tube

This project will leverage design approaches currently employed in existing shoulder launched weapon systems. The objective is to develop a common launch tube (CLT) for the Navy SPIKE weapon capable of being utilized with both a shoulder launcher and a multi-missile surface launcher. The SPIKE missile is being designed to be shipped/stored in a tube as an all-up round (AUR) that will be mounted mated either a shoulder launcher or multi-missile surface launcher for engagements. The goal is to have the same mechanical and electronic interfaces for both applications, so that only one AUR configuration is required for deployment.



Requirements

- DEPSECDEF Memo of Jan 23 2012 — USCENTCOM/ USPACOM Capability Enhancements
- COMUSFLTFORCOM NORFOLK VA 221715Z Sep 2011 — 2011 Fleet AT/FP IPCL
- CENTCOM JUONS CC-0506 — Smart Munitions for Aerostat Target Designation

Prevention

The security procedures taken to discourage an adversary from accessing weapons of mass destruction or gaining unauthorized access to critical assets are at the heart of prevention. This capability area focuses on broad spectrum, generic efforts that have the ability to influence multiple areas.

Requirements

- DoD S5210.41-M

Marine Mammal Enhanced Interdiction

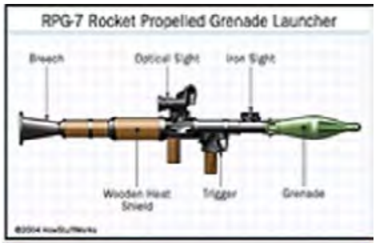
This project developed an Enhanced Interdiction Grabber that immediately stops an underwater intruder and allows the Swimmer Interdiction Security System to interdict multiple targets and hand off the intruder to a harbor security boat.

Stand-Off Weapon Defeat Integrated Product Team

This project will maintain a Joint Integrated Product Team (IPT) to support the development of a Stand Off Weapons (SOW) Defeat capability that was established under Phase 1 of the project in FY 14. The IPT is assessing current state of the art in SOW defeat capabilities then addressing the requirements, architecture, technology roadmaps, and funding needed to develop the capability.

Requirements

- DoD S5210.41-M - Volume I; Encl (5); Paragraph 2.e.



STAND OFF WEAPON DEFEAT
JOINT INTEGRATED PRODUCT TEAM

Storage & Safeguards

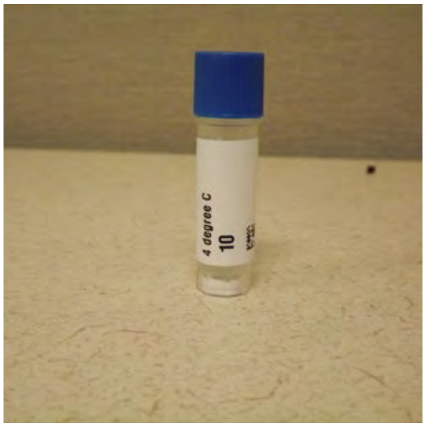
Properly securing critical assets to prevent access by unauthorized persons and implementing control measures that ensure access is limited to authorized persons is the foundation of physical security. This capability area focuses on equipment (e.g., locks, doors) designed to delay or stop unauthorized entry / access to a specified / localized area.

Requirements

- Inventory and accountability requirements from 42 CFR Part 73, 9 CFR Part 121, 7 CFR Part 331, DoD 5210.88/89, AR 50-1, and AR 190-17

Radio Frequency Identification Tagging for Items in Extreme Cold Storage

Determine if radio-frequency identification in extreme cold temperatures can track, identity, and ascertain the location of assets. This project improves physical security, inventory, and accountability of infectious agents and toxins.



APPENDICES

List of Acronyms

Acronym	Definition
APP	Application
AR	Army Regulation
ASN (EI&E)	Assistant Secretary of the Navy - Energy, Installations & Environment
AT&L	Acquisition, Technology, and Logistics
AT/FP	AntiTerrorism/Force Protection
AUR	All-Up Round
CBRN	Chemical, Biological, Radiological and Nuclear
CBRNE	Chemical, Biological, Radiological, Nuclear, Explosive
CCDE	Command & Control Display Equipment
CDD	Capability Development Document
CFR	Code of Federal Regulations
CNT	Countering Nuclear Threats
COMUSFLTFORCOM	Commander, U.S. Fleet Forces Command
CONOPS	Concept of Operations
CONUS	Continental United States
COTS	Commercial Off-The-Shelf
CPD	Capability Production Document
CWMD	Countering Weapons of Mass Destruction
DEPSECDEF	Deputy Secretary of Defense
DHHS	U.S. Department of Health and Human Services
DHS	Department of Homeland Security
DIA	Defense Intelligence Agency
DoD	Department of Defense
DoDD	Department of Defense Directive
DoDI	Department of Defense Instruction
DOJ	U.S. Department of Justice
DOS	U.S. Department of State
DSEA	Defense Security Enterprise Architecture
DSED	Defense Security Enterprise Discovery
DT	Developmental Test
DTRA	Defense Threat Reduction Agency
EDE	Explosive Detection Equipment
EHSS	Electronic Harbor Security Systems
FFC	Fleet Forces Command
FP	Force Protection

Acronym	Definition
FPCON	Force Protection Conditions
FPE	Force Protection Equipment
FY	Fiscal Year
G-BOSS(E)	Ground Base Operational Security System (Expeditionary)
HAF	Headquarters, Air Force
HALLTS	Hailing Acoustic Laser and Light Tactical System
HQ	Headquarters
HQ AF/A4SX	Headquarters, Air Force
HQDA	Headquarters, Department of the Army
HSPD	Homeland Security Presidential Directive
IBDC2	Integrated Base Defense Command & Control
IBDSS	Integrated Base Defense Security System
ICD	Initial Capabilities Document
IEDD	Improvised Explosive Device Defeat
IEEE	Institute of Electrical and Electronics Engineers
IEPD	Information Exchange Package Document
IGSSR-C	Integrated Ground Security Surveillance Response–Capability
IPCL	Integrated Prioritized Capabilities List
IPL	Integrated Priority List
IPT	Integrated Product Team
IUBIP	Integrated Unit, Base, Installation Protection
IWS	Integrated Waterside Security
J10NSN	Nuclear Enterprise Support Directorate Nuclear Surety Division
JSEOD	Joint Service Explosive Ordnance Disposal
JUONS	Joint Urgent Operational Needs Statement
LWI	Land Water Interface
MA	Mission Assurance
MILOps	Military Operations
NATO	North Atlantic Treaty Organization
NAWCWD	Naval Air Warfare Center Weapons Division
NC	Notional Concept
NIEM	National Information Exchange Model
NSWC IHEODTD	Naval Surface Warfare Center, Indian Head Explosive Ordnance Disposal Technology Division
NTTP	Navy Tactics, Techniques, and Procedures
NUONS	Navy Urgent Operational Needs Statement

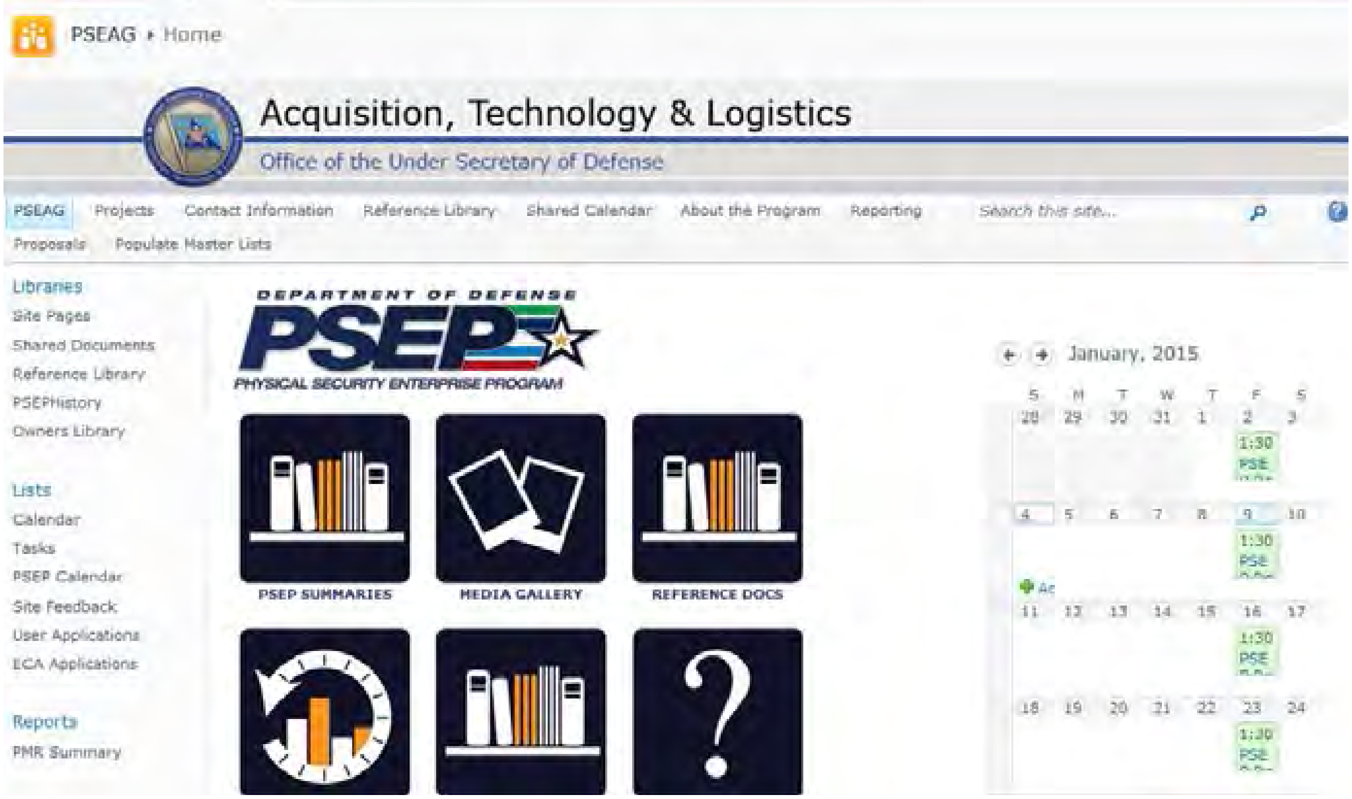
Acronym	Definition
OASD(NCB/CB)	Office of the Assistant Secretary of Defense for Nuclear, Chemical, and Biological Defense Programs: Chemical and Biological Defense
OASD(NCB/NM)	Office of the Assistant Secretary of Defense for Nuclear, Chemical, and Biological Defense Programs/Nuclear Matters
OCONUS	Outside the Continental United States
OOPMG	Office of the Provost Marshal General
OPNAV	Office of the Chief of Naval Operations
OPNAVINST	Office of the Chief of Naval Operations Instruction
POR	Program of Record
PSE	Physical Security Equipment
PSEAG	Physical Security Enterprise & Analysis Group
PSEP	Physical Security Enterprise Program
RDT&E	Research, Development, Test and Evaluation
RFI	Request for Information
SECDEF	Secretary of Defense
SECNAVINST	Secretary of the Navy Instructions
SEIWG	Security Equipment Integration Working Group
SIPRNet	Secret Internet Protocol Router Network
SME	Subject Matter Expert
SOW	Standoff Weapons
SPAWAR	Space and Naval Warfare Systems Command
SSP	Strategic Systems Programs
STIPL	Science and Technology Integrated Priority List
T&E	Test & Evaluation
TRADOC	Training and Doctrine Command
UONS	Urgent Operational Needs Statement
USAF	United States Air Force
USCENTCOM	United States Central Command
USEUCOM	United States European Command
USFFC	United States Fleet Forces
USMC	United States Marine Corps
USN	United States Navy
USNORTHCOM	United States Northern Command
USPACOM	United States Pacific Command
WNY	Washington Navy Yard
XML	Extensible Markup Language

Acquisition, Technology & Logistics
Office of the Under Secretary of Defense
PSEP-level Project Site
Shared Documents
DEPARTMENT OF DEFENSE
PSEP
PHYSICAL SECURITY ENTERPRISE PROGRAM
Projects

PSEAG Sharepoint Site

The Physical Security Enterprise & Analysis Group (PSEAG) developed a web portal (right) that will allow program managers, government representatives, support contractors and other approved users to access a wealth of Physical Security RDT&E-related information, upload reports, view PSEAG History projects and collaborate in a secured environment. The portal is designed to foster collaboration between force protection (FP) communities. In addition, it promotes and allows the collection, organization, and dissemination of information to its members. All registered portal users are able to access information and studies on the latest FP equipment and on policy documents that provide guidance on the development and use of physical security equipment.

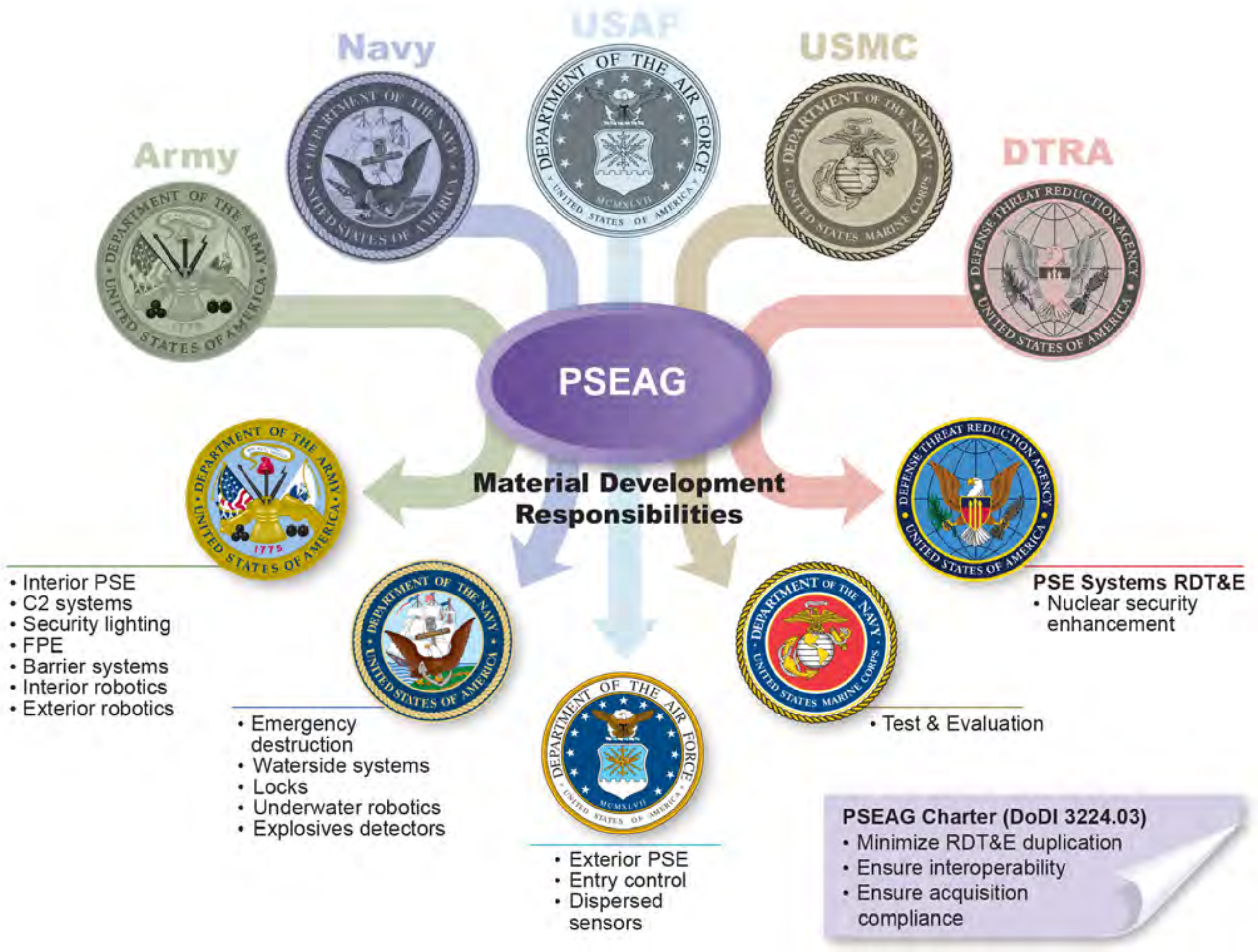
This tool modernizes the once tedious paper process and standardizes the format for all future projects. The web portal also allows for users to enter monthly reporting and scheduling data for projects, from which the system will generate reports and display project health information for use by managers and in conducting project reviews. The system will also become an archive of project data and a useful tool for referencing old projects and reporting on historical data.



DoD Physical Security Enterprise & Analysis Group

PSEAG Organization and Structure

The Physical Security Enterprise & Analysis Group (PSEAG) is composed of primary voting members from the Services and the Defense Threat Reduction Agency (DTRA), with a complement of advisory personnel from the Joint Staff, other Deputy Assistant Secretaries of Defense, the Defense Intelligence Agency (DIA), the Department of Energy, and other Federal agencies. Oversight of the PSEAG is executed by the Office of the Assistant Secretary of Defense for Nuclear, Chemical, and Biological Defense Programs/Nuclear Matters (OASD(NCB/NM)).



- Interior PSE
- C2 systems
- Security lighting
- FPE
- Barrier systems
- Interior robotics
- Exterior robotics

- Emergency destruction
- Waterside systems
- Locks
- Underwater robotics
- Explosives detectors

- Exterior PSE
- Entry control
- Dispersed sensors

- Test & Evaluation

PSE Systems RDT&E
- Nuclear security enhancement

PSEAG Charter (DoDI 3224.03)
- Minimize RDT&E duplication
- Ensure interoperability
- Ensure acquisition compliance